Internet Commerce Coalition

April 11, 2008

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles

Dear Secretary:

The Internet Commerce Coalition appreciates the opportunity to respond to the Commission's Proposed Self-Regulatory Principles ("Principles") for Online Behavioral Advertising. We commend the Commission for its work raising awareness of behavioral advertising and its support for self-regulation, but believe that the Principles should be clarified substantially and perhaps be subject to another round of public comment before being finalized.

The Internet Commerce Coalition includes leading Internet Service Providers, e-commerce sites and technology trade associations. Members include Amazon.com, AT&T, Comcast, eBay, ITAA, Monster.com, Verizon, and the U.S. Telecom Association. The ICC works for reasonable rules governing liability and regulation of technology that will allow e-commerce and communications technology to flourish.

With regard to behavioral advertising, ICC members work to educate users regarding collection of information online, and particularly appreciate the Commission's focus on this issue.

We strongly support the Commission's goal of enhancing self-regulation in the area of behavioral advertising, and agree with the Principles' goals of educating consumers about online tracking, giving consumer control over uses of sensitive information, and securing data to prevent potential misuse, but believe that the Principles should be clarified and realigned with actual consumer harm.

A. General Comments on the Principles

We note at the outset that the purpose of self-regulatory principles is to encourage self-regulation. For this reason, the Commission's Principles will achieve their highest purpose by stimulating and reflecting self-regulatory practices that prevent harm to consumers, and that continue to adapt to changes in technology and consumer demands. In the end, there may be no need for "Final FTC Principles."

500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000

Second, we note that it is difficult to comment in detail on the Principles because, as set forth in the Commission's Staff Statement, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*,[1] the scope of the Principles remains quite unclear. For example, it is unclear: (1) what "concerns" the Principles are designed to address,[2] (2) whether those concerns are in fact grounded in actual practices that harm consumers, (3) what sorts of tracking the Principles would cover (*e.g.*, tracking within a site or family of sites, maintaining a web log for network management purposes), (4) what entities would be subject to the Principles, (5) whether the Principles would cover personally identifying information ("PII") or non-PII as well, (6) whether the individual proposed Principles should be read literally or as broad goals to be fleshed out in self-regulatory programs, and (7) how the Principles would operate in combination with other regulatory and self-regulatory systems.

Because these questions are all fundamental to evaluating the Principles, if the Commission decides to move forward to finalize any Principles other than those endorsed by self-regulatory organizations, we respectfully suggest that it put that more specific proposal out for further comment on a shorter comment deadline.

It is also far from clear that "behavioral advertising" itself – as opposed to the use or disclosure of sensitive data about individuals – is a privacy issue. For this reason, we suggest that the Commission may want to use terminology that reflects a focus on data practices in connection with advertising, rather than advertising *per se*.

As the Staff Statement recognizes at p. 2, behavioral advertising on the Internet provides significant benefits. It is central to the availability of free, quality content on the Internet and to useful comparative advertising. It is also designed to provide Internet users with ads that they are more likely to be interested in, and fewer ads that are not of interest.

Nor is behavioral advertising a new phenomenon. For example, direct marketers use offline behavioral information and census data to refine and target their offline marketing efforts. TV and magazine advertisers, of course, study the demographics of audiences of the medium on which they advertise, and even purchasers of roadside billboard space know the location of their audience and the direction they are driving in.

Singling out behavioral advertising on the Internet for restrictions that do not address consumer harm would effectively discriminate against Internet commerce and would make it a less viable source of valuable, free information and value-added services that consumers have come to expect and rely upon. It would be discriminatory and highly anomalous to suggest a

---

[1] Available at http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[2] By way of example, the Notice asks "(1) which secondary uses raise concerns" and "(2) "whether companies are in fact using data for these secondary purposes." Staff Statement at 6. Without a clear understanding of what would give rise to concerns, it is difficult or impossible to answer the critical question whether data are being used for objectionable purposes.

self-regulatory regime for behavioral advertising that is far more extensive than existing *regulatory* regimes that apply online and offline.

B. Definition of Behavioral Advertising

The definition of "behavioral advertising" set forth on p.2 of the Staff Statement appears to define behavioral advertising in a broad manner and could cover advertising models that are not based on users' behavioral patterns at all. For example, the definition appears to cover collection of data for dual uses – for purposes such fraud prevention, user authentication or improving service, *and* advertising. These are surely not the sort of "secondary uses" that the Staff suggests may cause concern, and if final Principles are issued, they should be clearly exempt.

The scope of the Principles would preclude any one-size-fits-all approach for self-regulation, and necessitates approaches that are flexible and leave room for innovation. At the same time, the Principles should not create an artificial advantage (for example, by requiring more onerous notice) for one type of behavioral advertising business model over others.

We believe that a primary focus of the Principles should be on situations in which there is no direct relationship between the consumer and the entity collecting and using behavioral advertising data.

Consumers have far less visibility into the practices of entities, such as network advertisers, with whom they are not in direct privity of contract. Consumers do not sign up for service with these third party service providers, do not "log into" these service providers' networks, and do not typically have occasion to visit their home pages to check their privacy policies. Likewise, these third parties are far less likely to be subject to consumer pressure regarding their privacy practices.

The definition of "behavioral advertising" refers abstractly to "tracking." It thus would apply to tracking user activities within a single website or family of related websites to customize and improve web content or to show users what e-commerce products or job listings they have previously examined. These are beneficial uses of data that consumers fully expect and that should not be covered by the Principles.

Such consumer interactions with entities that the user has a direct relationship with are anticipated by consumers and are addressed in privacy policies that are available to users at the time they sign up for service or at the footer of a website's home page. Furthermore, ISPs and e-commerce sites operate in highly competitive environments. If they pursue aggressive policies that consumers object to, they risk losing customers, which directly affects the utility of their advertising programs and revenue bases. By contrast, consumers have far less visibility into the practices of third parties engaged in behavioral advertising.

For all these reasons, we believe that the proposed Principles should focus particularly on situations in which entities with whom a consumer does not have a direct relationship use behavioral advertising data. This could be accomplished in the definition of "behavioral advertising" or elsewhere in the Principles.

C. Personally Identifying Information

The Staff Statement's proposed definition of "behavioral advertising" is silent as to whether it applies to non-personally identifying data. However, its abstract reference to "tracking" read literally would, for example, reach non-personally identifying log-file data routinely used by websites and related destinations on the Internet. Furthermore, the Staff Statement asks "whether concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data." (Statement at 6).

To our knowledge, no federal privacy law or regulation applies to non-personally identifying information. It would be highly anomalous to suggest more extensive self-regulation of such data than, for example, HIPAA or GLB regulation of non-personally identifying financial or health information. Furthermore, applying the full panoply of proposed Principles to non-personally identifying information would have the perverse effect of *removing incentives for companies to keep behavioral advertising data in non-personally identifying form* when today most Internet advertising is conducted without using PII at all.

The key question for purposes of the FTC's inquiry should be whether data *has become personally identifying*, and to create incentives for entities to keep data in non-personally identifying form. Furthermore, the fact that information *might be* converted into personally identifying form does not mean that it should be treated as personally identifying when a service provider has made a concerted effort and avoided using the information in personally identifying form.

We understand that some Commission staff question the continued viability of the PII/non-PII distinction, pointing to the advent of IPv6 IP address assignment data. It is important to understand that even IPv6 addresses will be masked for users accessing the Internet behind an Ethernet connection, a Blackberry device or a variety of other connections. Furthermore, even if such addresses include media access control (MAC address) information, they simply indicate that a particular machine is accessing the Internet without revealing the identity of the Internet user or distinguishing multiple users of the same machine (for example, different family members) from each other.

Opponents of the PII/non-PII distinction further argue that in some circumstances users may make their name part of behavioral advertising data, for example, by conducting a Google search on their name. Even if the text of these types of search queries is provided to network advertisers, it would not be possible for an advertiser to discern whether such information in fact relates to the owner of the computer in question, rather than someone else.

To the best of our knowledge, other scenarios that assume that IP address information is or will become personally identifying in the behavioral advertising context are speculative.

However, formulating the Principles to eliminate the distinction will only make this speculation a self-fulfilling prophecy. If it wants to enhance privacy in the IPv6 world, the Commission would do far better to preserve the PII/non-PII distinction in its Principles and thereby create incentives for Internet businesses to avoid keeping this information in personally identifying form.

We believe that while the consumer notice, data security Principles make sense to apply to non-personally identifying information, the other Principles do not, with the exception of a very limited amount of sensitive information discussed in the section D. 4. below.

D. Specific Principles

1. Transparency and Consumer Control

While we suspect that most consumers are now aware of the use of behavioral advertising data to target ads on free properties on the Internet, we agree that greater transparency of data collection for behavioral advertising is desirable.

The proposed Principle on this subject suggests that "every website" collecting information for this purpose "should provide a clear, concise, consumer-friendly and prominent statement" that data is being collected for advertising. We believe that this Principle can work, provided that the information is furnished through a hyperlink, for example, to clear language in a privacy policy or in the bottom of an ad.

We disagree, however, that final Principles should specify that websites should provide "a clear, easy-to-use, and accessible method" for consumers to opt-out of non-personally identifying information. (Statement at 3). As discussed above, this option is not available to consumers even for personally identifiable information in most offline contexts and provided that the information is not used actually to identify a consumer, it should not raise privacy concerns.

However, if the information is used to identify an individual, then the Staff's consumer control Principle should apply.

2. Reasonable Security and Limited Data Retention

There is no evidence that the one breach of search data that forms the basis for the assertion that, "[s]takeholders express concern that [behavioral advertising data] . . . could find its way into the hands of criminals or other wrongdoers," (Statement at 4) resulted in any harm whatsoever. Nevertheless, we agree that it is important to implement appropriate security measures for behavioral advertising data. Companies have a strong market incentive to do this already, but including it in best practices principles would be helpful.

With regard to data retention periods, service providers already carefully calibrate how long they retain data and retain the information for legitimate business purposes. Given the wide array of business models, and potentially even industry sectors, covered by the Principles, we do not believe that the Principles can address retention periods more specifically than currently set forth in the Staff Statement.

3. Affirmative Express Consent for Material Changes

The Staff Statement's proposal for "affirmative express consent" for changes in uses of data (Statement at 5) could create a very significant distinction for companies to adhere to the Principles and rests on a misinterpretation of the *Gateway Learning* consent decree.

If changes with regard to non-personally identifying uses of behavioral advertising data – which, as explained above, are often collected for multiple beneficial purposes – trigger an opt-in consent requirement, it would slow innovation in Internet services and may discourage companies from signing up to follow the self-regulatory system.

Furthermore, *Gateway Learning*, Dkt. No. C-4120 (Sept. 10, 2004), did not indicate, as the Staff Statement appears to assume, that material changes in *any* sort of data use practices trigger an opt-in requirement. On the contrary, *Gateway Learning* involved a company that promised (1) *never* (2) to *disclose* (3) *personally identifying information* unilaterally changing its policies to disclose the personally identifying data. *None* of these three conditions are mentioned in this proposed Principle. Rather, it appears to assume that entities that have not made strong promises, are not disclosing the data at all, and that are handling data in non-personally identifying form, should obtain affirmative consent before changing their uses. In fact, far from suggesting this sort of rigid rule, *Gateway Learning* suggests a "sliding scale" under which notice, notice and opt-out, and affirmative consent may be required in different circumstances.

Both for practical purposes of encouraging participation in this self-regulatory effort, and to avoid an abrupt and anti-Internet discriminatory lurch in FTC policy regarding changes in data use, we respectfully suggest that this Principle be dropped, or that it be limited to information used in personally identifying format and reflect the sliding scale approach in *Gateway Learning.*

4. Sensitive Data

The Staff Statement asks (at p.6) "what classes of information should be considered sensitive" and whether uses of this information for behavioral targeting should be banned entirely.

We agree that there is a very limited amount of information – specifically information regarding a user's sexual orientation, sexual life, or medical conditions – that is so sensitive that it should not be used for behavioral advertising without offering consumers clear notice and the opportunity to refuse its use for behavioral advertising. Robust consumer choice is important in this context because presenting targeted advertising on these subjects presents a risk of revealing sensitive information to other users of the same computer.

On the other hand, some consumers may specifically desire advertising based upon these criteria, therefore consumer choice, rather than an outright ban, is appropriate.

5. Secondary Uses

We agree strongly that non-personally identifying tracking data collected for advertising purposes is also used to improve website content, products and services. (Statement at 6).

As discussed in the General Comments section of this Comment letter, it is extremely difficult to comment on "potentially harmful" secondary uses of behavioral advertising data (Statement at 6), absent any specification of what those uses are thought to be. At this juncture, the ICC and its members are not aware that such nefarious uses are occurring. However, this

would be an appropriate subject for further comment if the Commission identifies problematic secondary uses.

We thank you for considering our views, and are eager to continue to work with you in a constructive fashion to help refine self-regulatory principles in this area.

Sincerely,

Jim Halpert
General Counsel

Internet Commerce Coalition
500 8th Street N.W., Washington, D.C. 20004
tel: 202.799.4000 fax: 202.799.5000